

In re Application of: Shelest et al.
Application No.: 10/010,352

Remarks

In the application, claims 1 through 17, 21, and 22 are pending. No claims currently stand allowed.

The Office Action dated October 1, 2004, has been carefully considered. The Office Action provisionally rejects claims 1 through 22 under the judicially created doctrine of obviousness-type double patenting as obvious over the combination of various claims pending in U.S. Patent Application 09/833,922 (the parent of the present application) and U.S. Patent RE 36,946 ("Diffie"). Claims 1 through 22 are also rejected under 35 U.S.C. § 102(e) as anticipated by Diffie.

In order to expedite the prosecution of the currently pending claims and to overcome the obviousness-type double patenting rejection, Applicants submit with this Amendment B a terminal disclaimer.

The present application and Diffie are both directed towards methods of using encryption to secure information sent over a network in the presence of possible eavesdroppers. However, the specifics of the presently claimed invention go beyond the teachings of Diffie in several respects. In claim 1, for example, the following highlighted elements are not discussed in Diffie:

1. A method for a first computing device to make authentication information available to a second computing device, the method comprising:
creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device, and a digital signature, *the network address having a portion derived from the public key of the first computing device*, the digital signature generated by signing with a private key of the first computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data; and
making the authentication information available to the second computing device, in part by sending a message to the second computing device, *the message including the digital signature in a packet option*.

(Emphasis added.) (Claim 2 contains identical language.) The sections of Diffie cited against these elements of claim 1 discuss various types of authentication information, but they do not discuss a network address addresses derived from a public key (or derived from anything else,

In re Application of: Shelest et al.
Application No.: 10/010,352

for that matter). Neither does Diffie discuss the use of a packet option to transmit a digital signature. These aspects are neither anticipated nor rendered obvious by Diffie, and thus claims 1 and 2 are patentable over Diffie. Similarly, Diffie does not teach the somewhat similar elements of claim 3:

3. A method for a second computing device to authenticate content data made available by a first computing device, the method comprising:
 - accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature;
 - deriving a portion of a second network address from the public key of the first computing device;*
 - validating the digital signature by using the public key of the first computing device; and
 - accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data,*
 - wherein the second computing device accesses the public key of the first computing device over an insecure channel, and wherein if the content data are not accepted, then the public key is discarded.

(Emphasis added.) (Claim 5 contains identical language.) Claims 6, 8 through 11, 17, and 21 all contain at least one element similar to the ones highlighted above and are therefore patentable over Diffie for the same reasons.

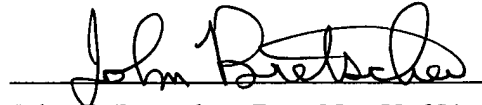
All other pending claims depend upon one or the other of these independent claims. Therefore, all pending claim are patentable over Diffie at least for the reasons given above.

In re Application of: Shelest et al.
Application No.: 10/010,352

Conclusion

The application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,

A handwritten signature in black ink, reading "John T. Bretscher", is written over a horizontal line.

John T. Bretscher, Reg. No. 52,651
One of the Attorneys for Applicants
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza, Suite 4900
180 North Stetson
Chicago, Illinois 60601-6780
(312)616-5600 (telephone)
(312)616-5700 (facsimile)

Date: November 24, 2004